PROJECT
ENG
PRO

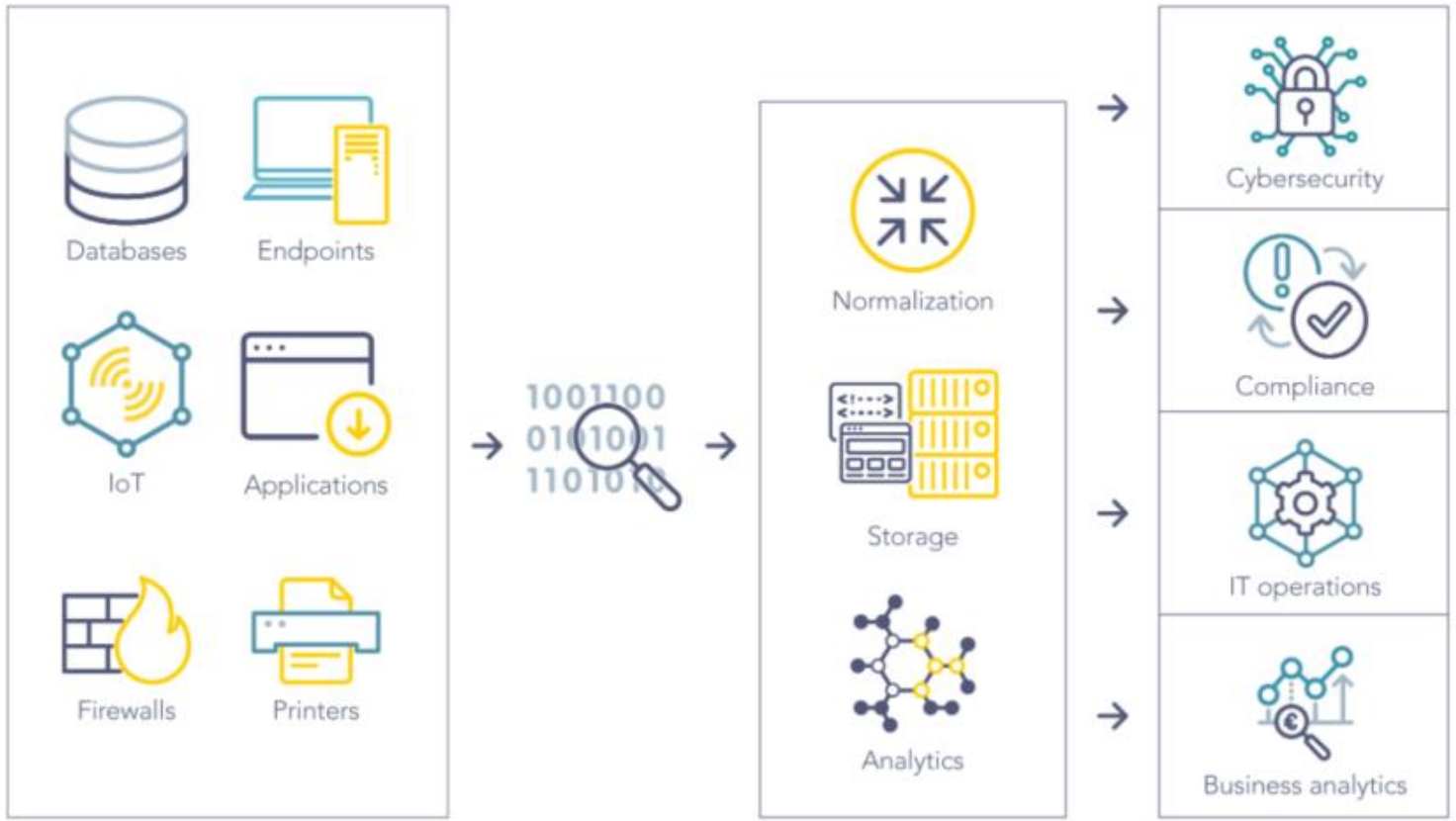
CYBER SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

By Project ENG PRO

SIEM Solutions in Cybersecurity

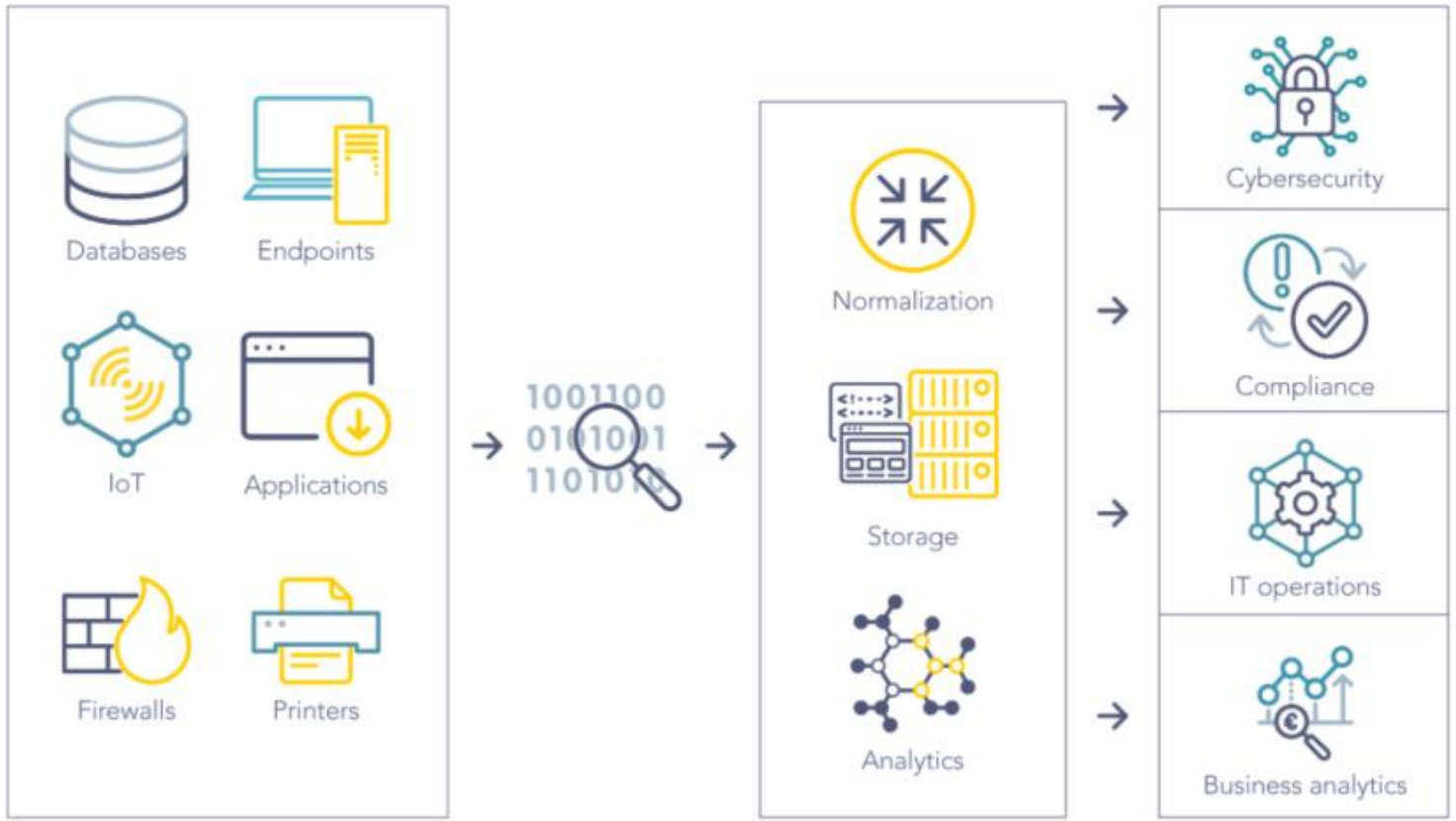
SIEM Introduction

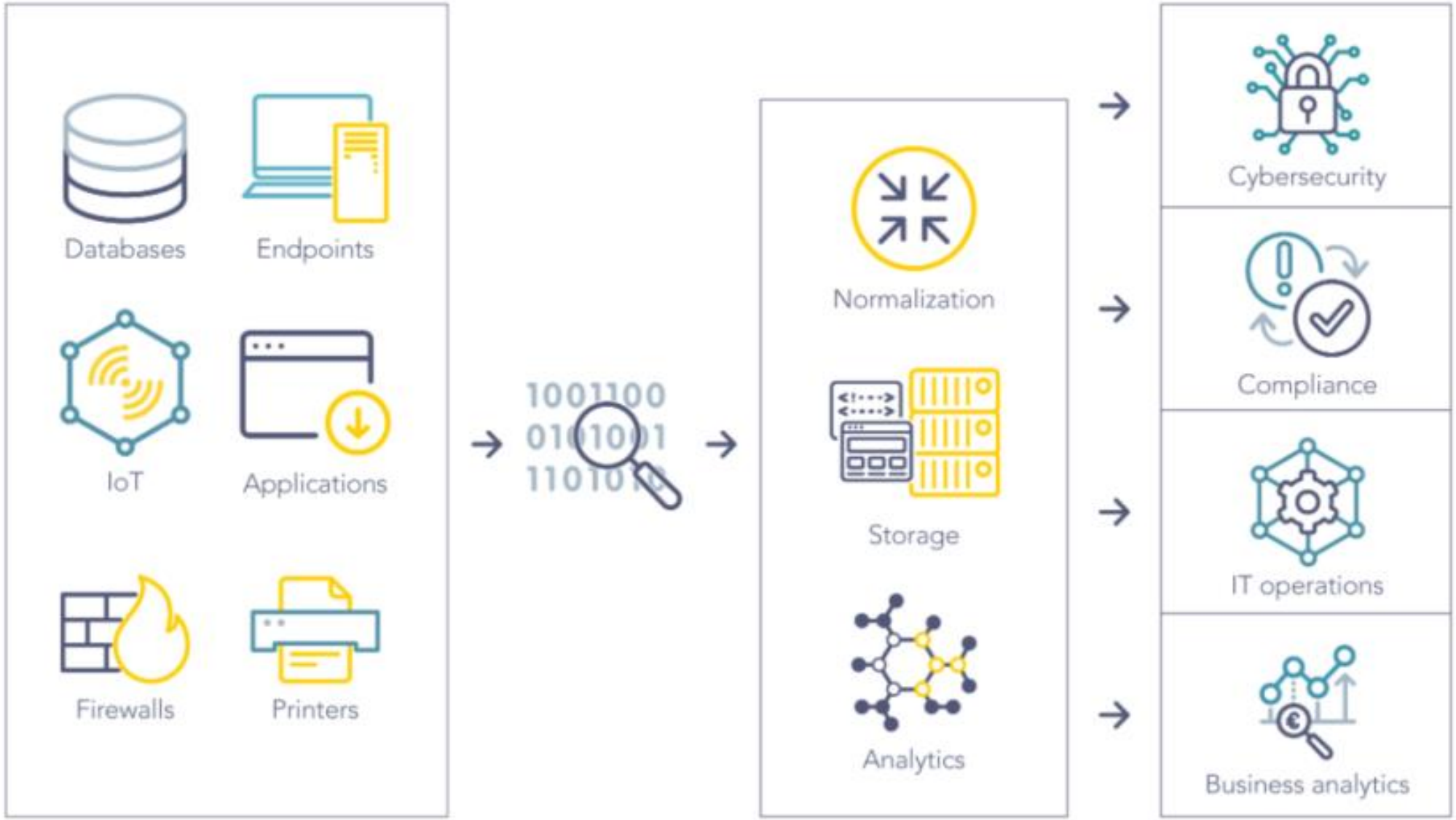
SIEM software collects and aggregates log data generated throughout the entire IT infrastructure, from cloud systems and applications to network and security devices, such as firewalls and antivirus.



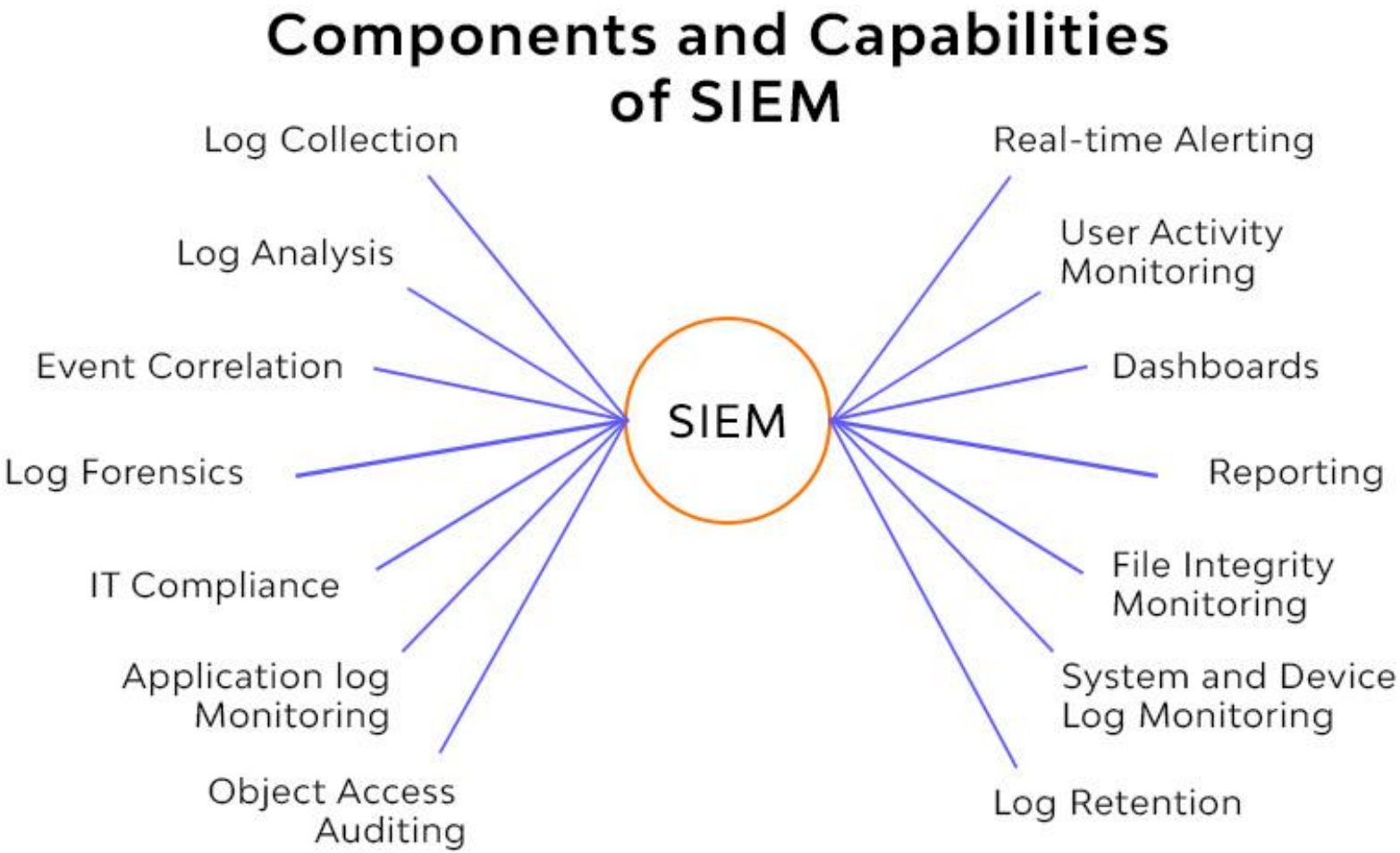
SIEM Introduction

Enterprises must monitor and guard their data to protect themselves from increasingly advanced cyber threats in the digital economy. Companies have more data to collect and analyze than ever before.





Log Management



Log Management's Broad Scope

SIEM's Analytical Power

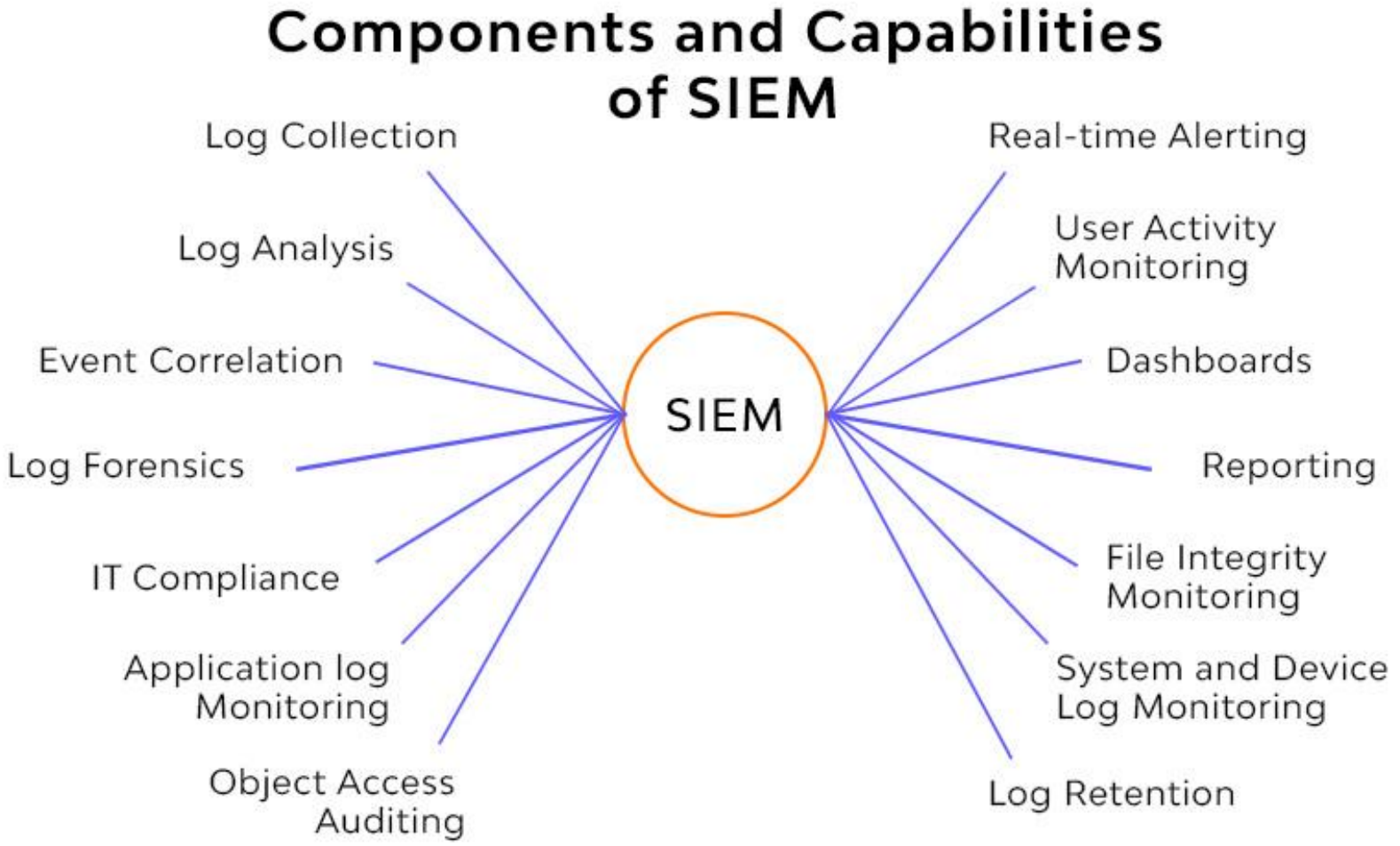
Centralized Insights

Alerting

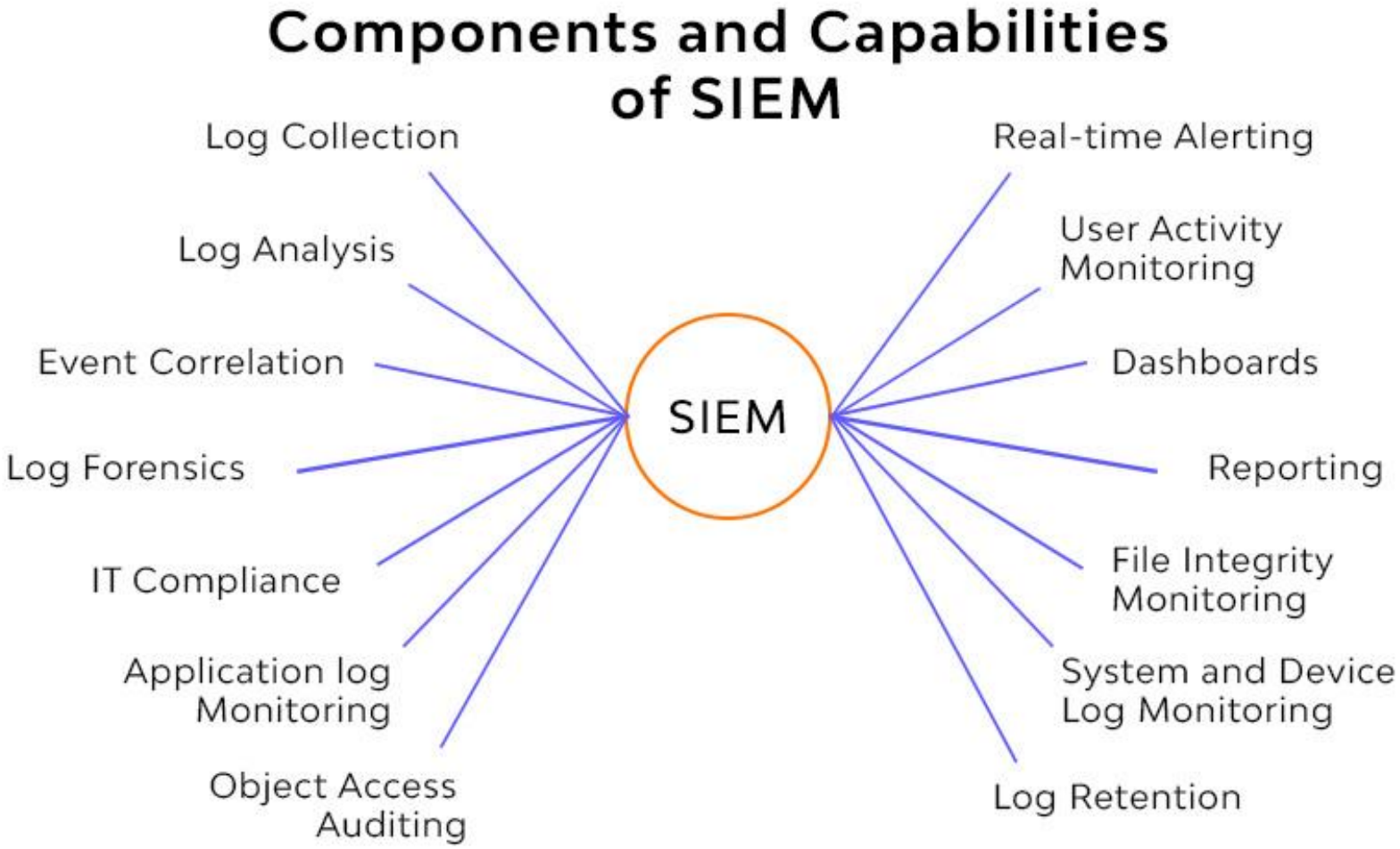
Analyzing Events

Escalating Alerts

Notifying Security Staff



Dashboards and Visualisation



Dashboard and Visualization

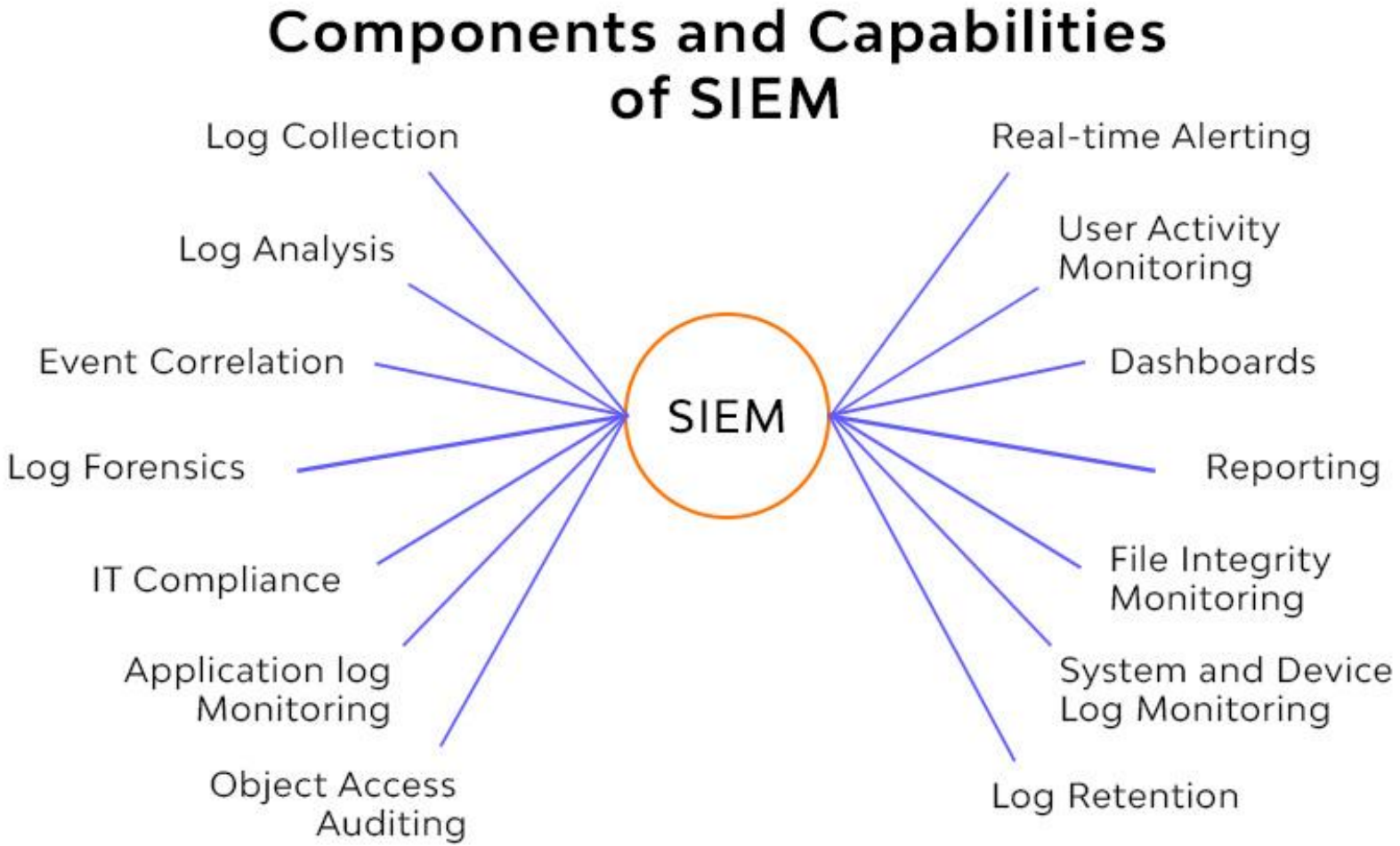
Pattern Identification

Data Retention

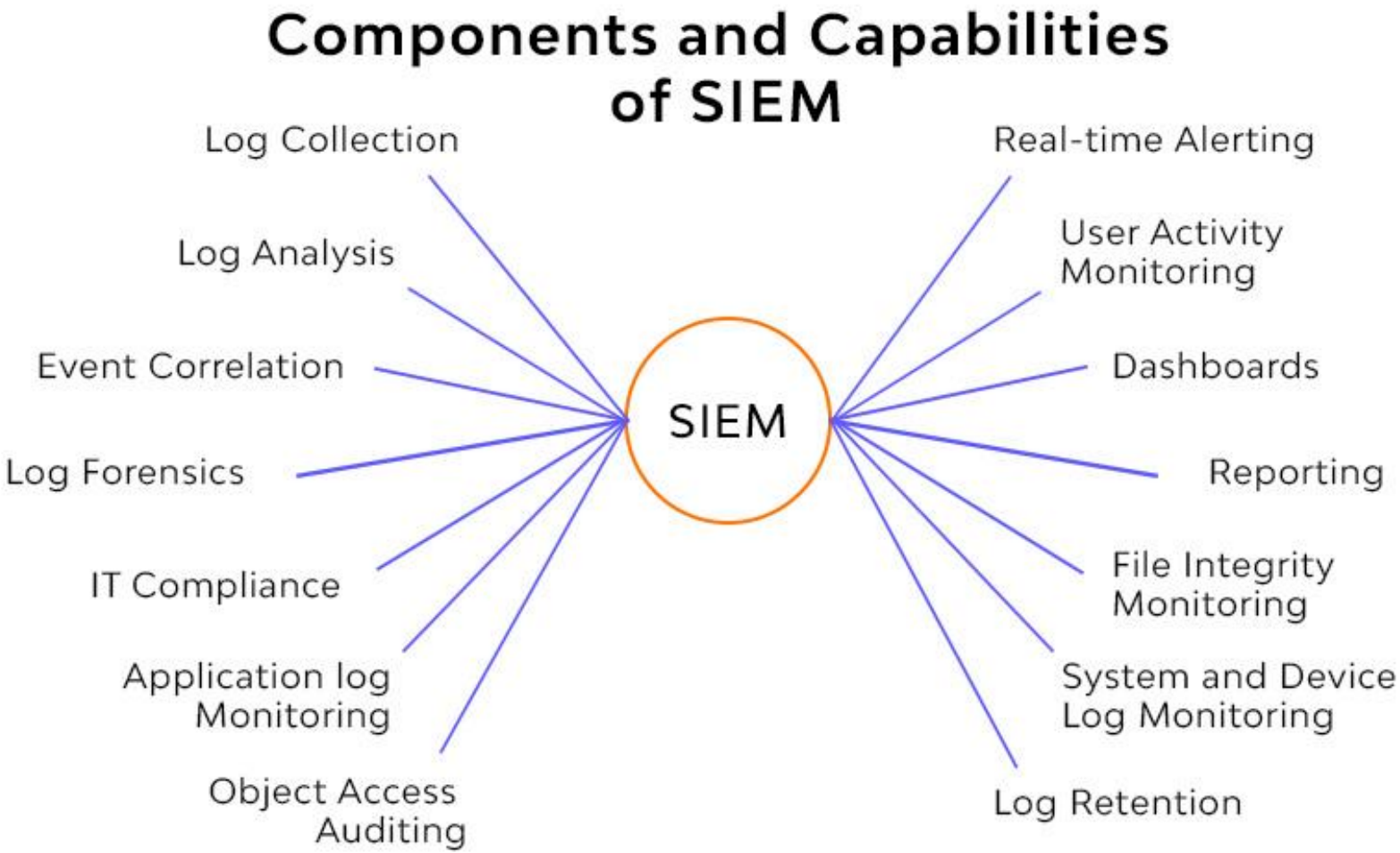
Date Retention

Storing Historical Data

Supporting Forensic Investigations



Threat Hunting



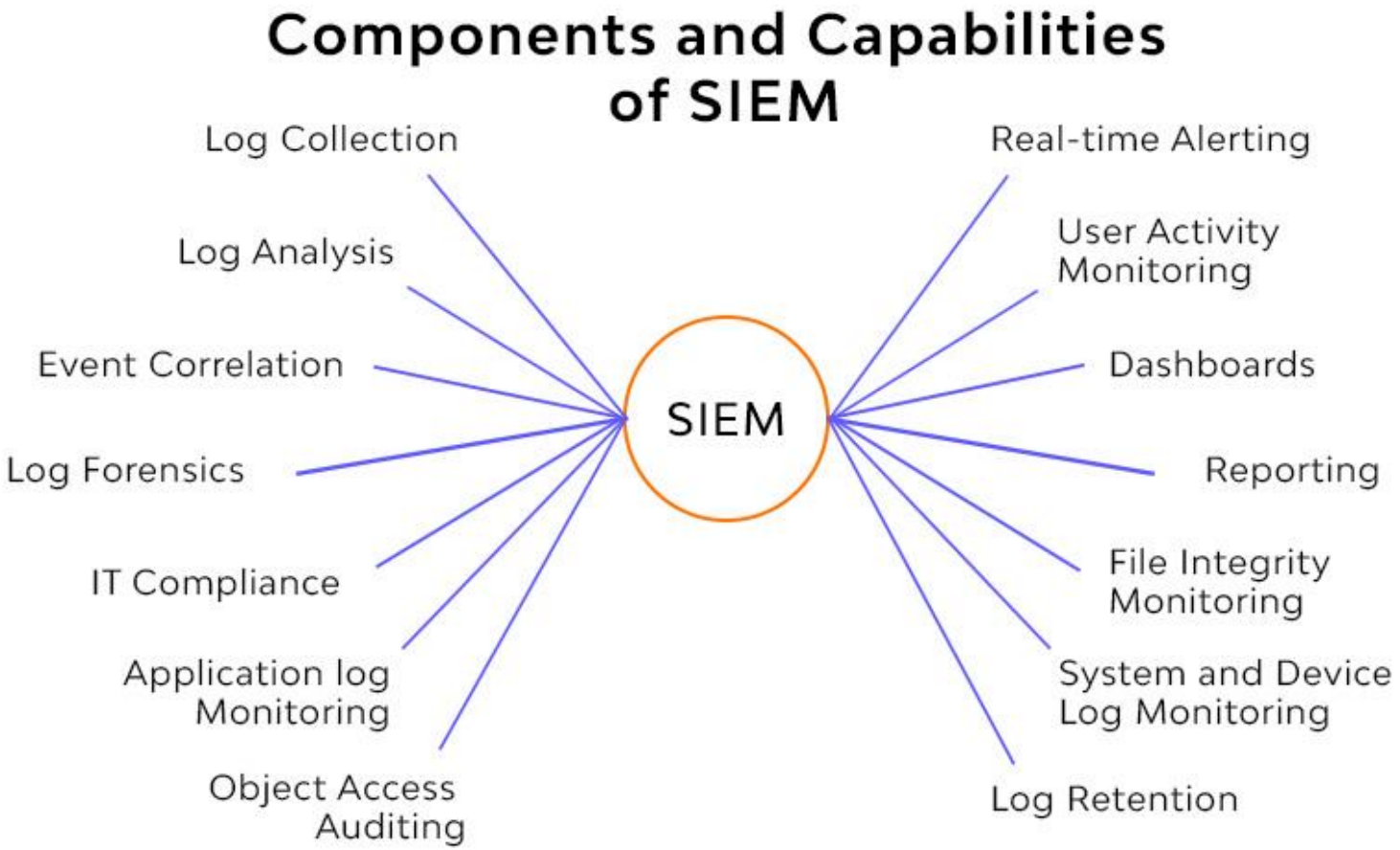
Proactive Threat Hunting

Manual or Automated

Query and Analysis

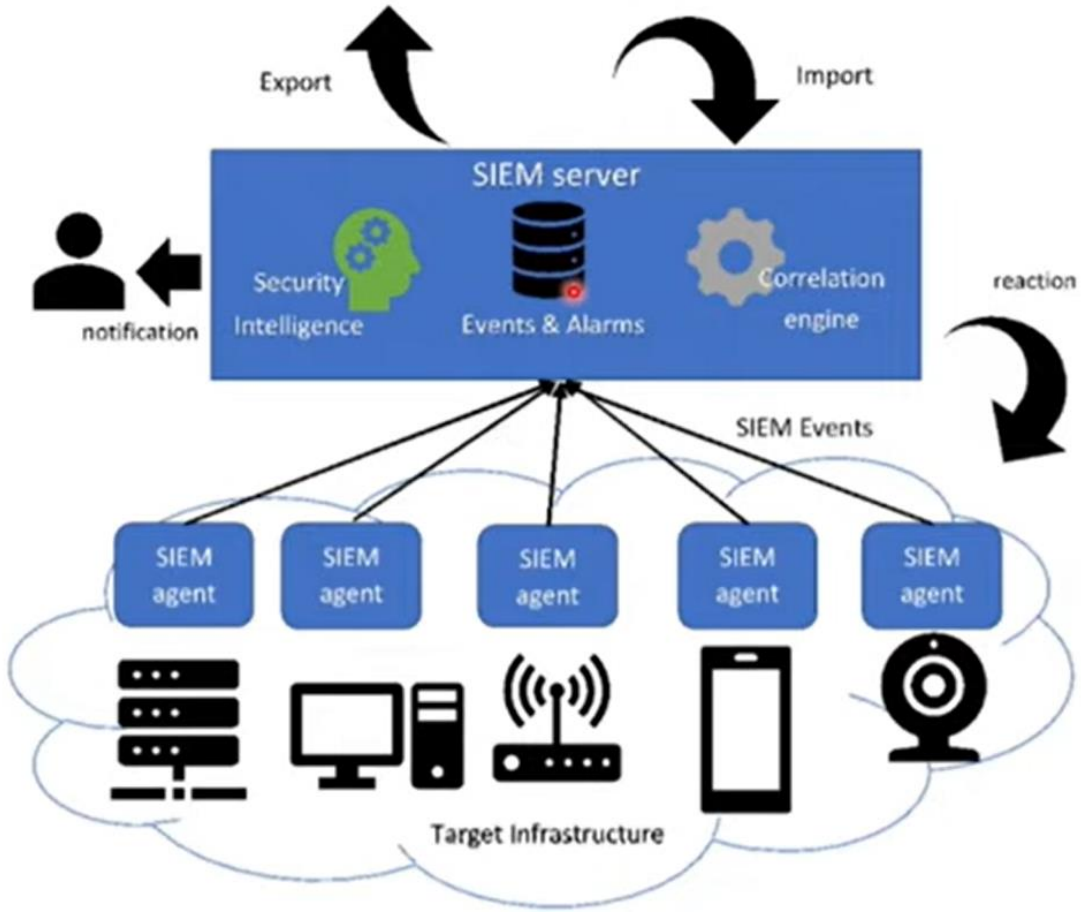
Incident Response

- Case Management and Collaboration
- Knowledge Sharing
- Integration with Ticketing Solutions
- Communication Tool

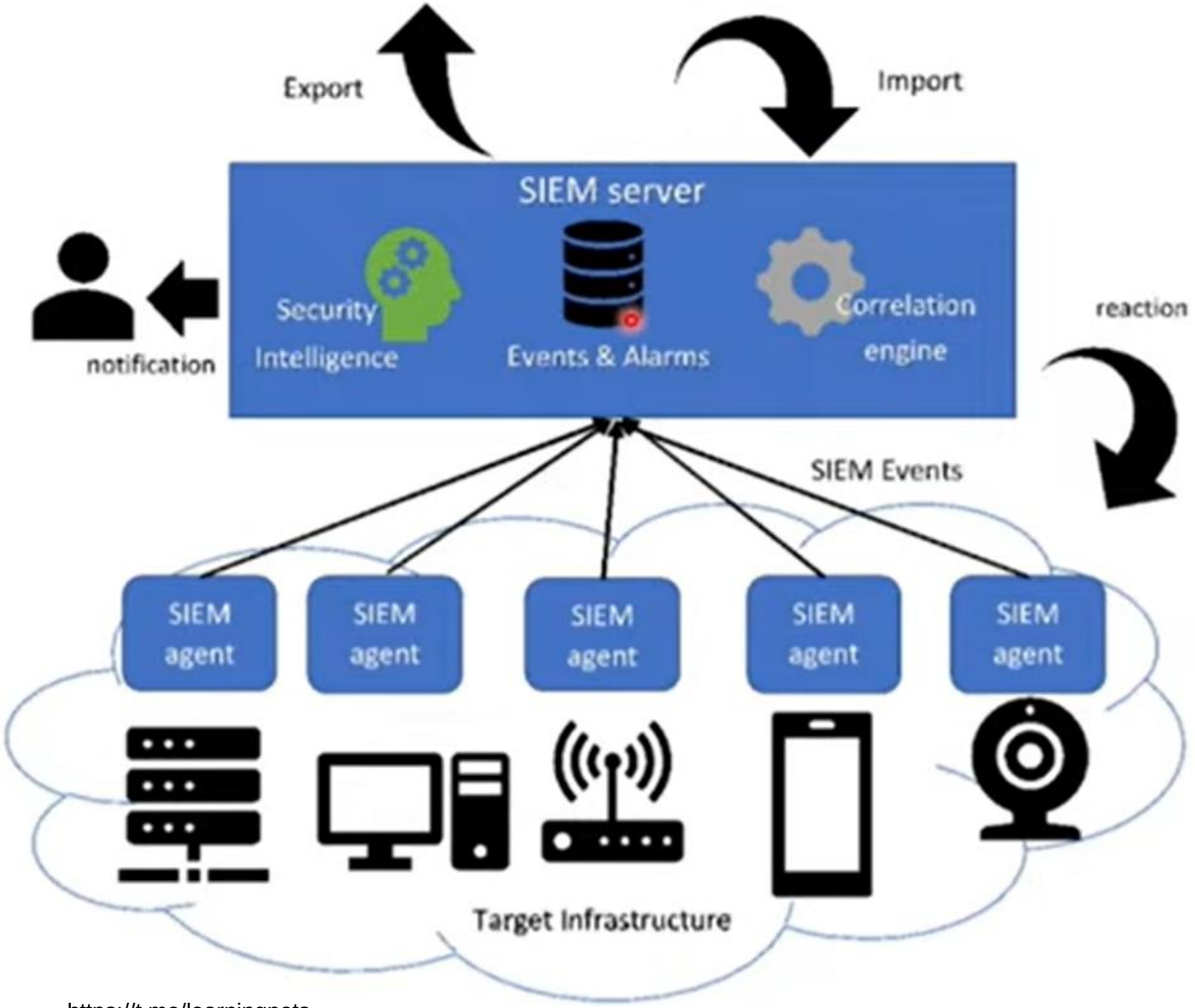


SIEM Solutions

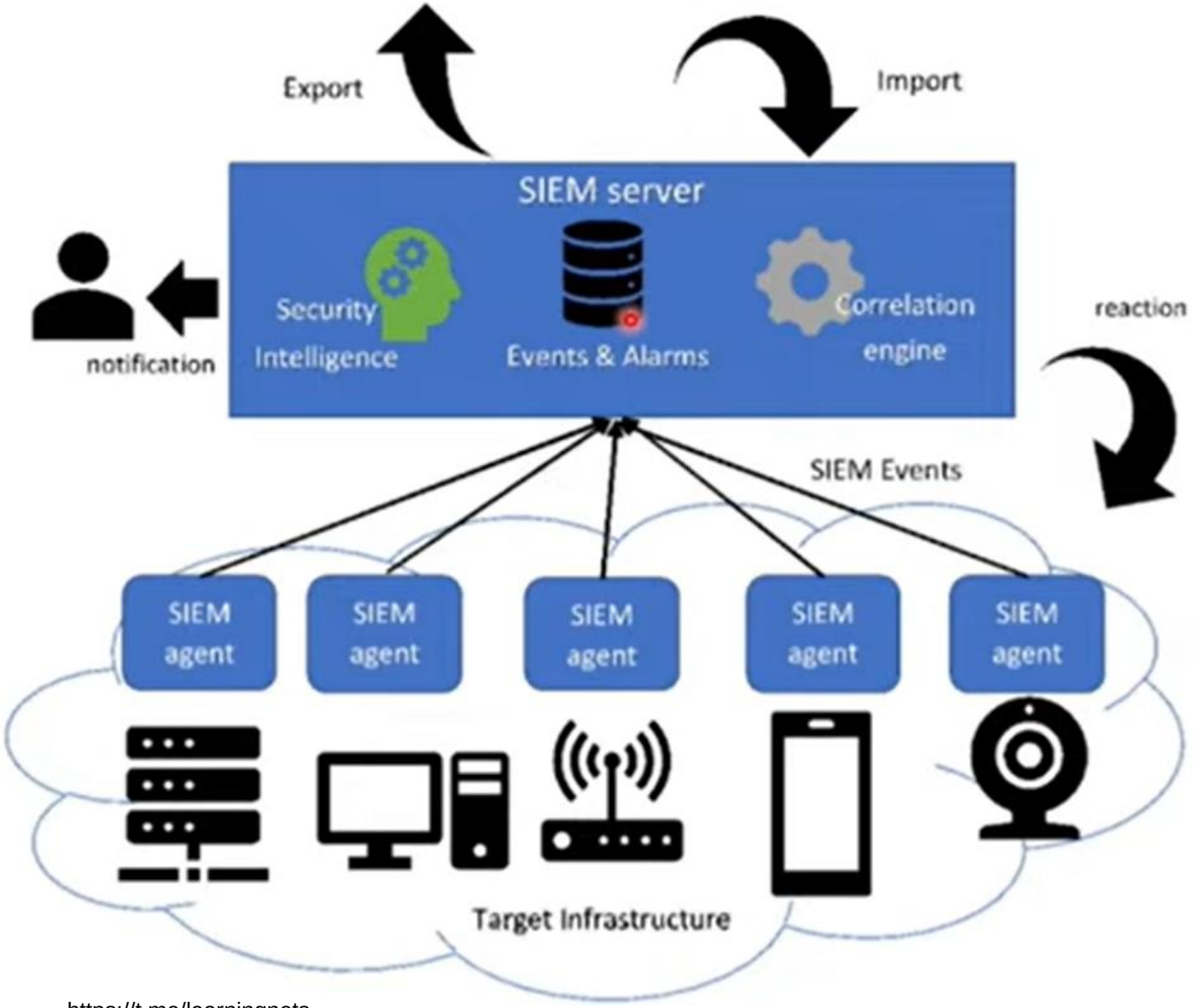
There's a variety of SIEM (Security Information and Event Management) solutions available in the market, including Splunk, Exabeam, LogRhythm, FortiSIEM, IBM QRadar, Secureworks, and even Elasticsearch with SIEM capabilities.

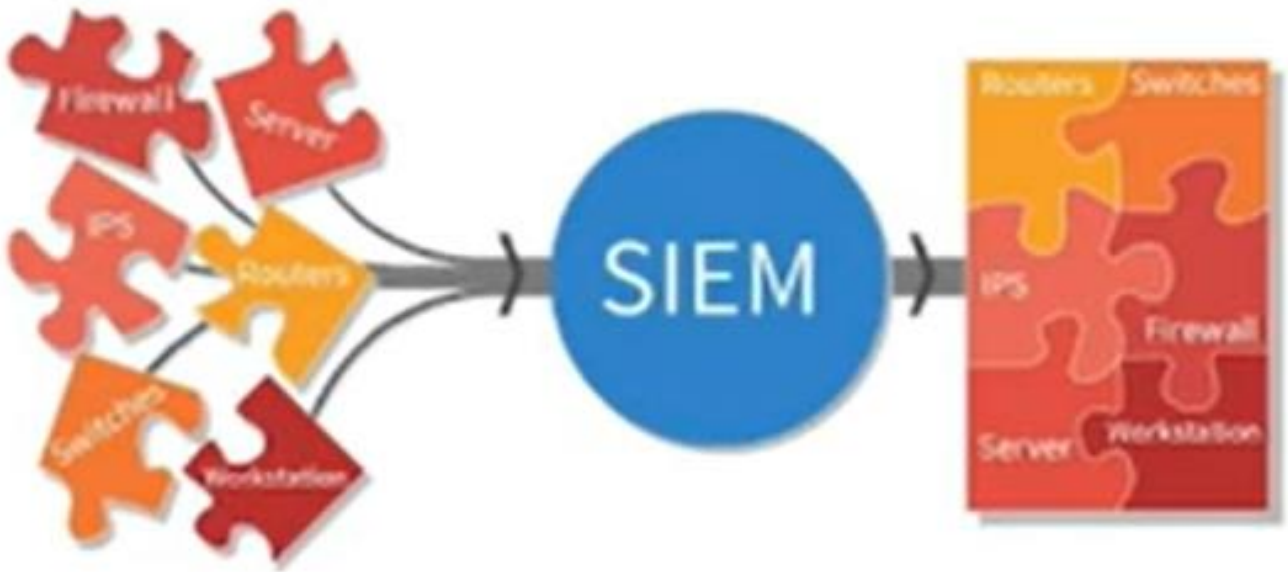


SIEM Solutions Deployment



SIEM Solutions Functional Components





Wrap Up